나무위키

# Zcash

최근 수정 시각: 2026-08-10 13:05:36

분류:암호화폐

**ZEC**는 여기로 연결됩니다. 롯데웰푸드의 과자에 대한 내용은 제크 문서를 참고하십시오.

GRAYSCALE
**그레이스케일 포트폴리오 암호화폐**
**[ 펼치기 · 접기 ]**

목차


1. 개요
2. 주소 유형
3. 지갑 소프트웨어
4. 익명성
5. Trusted Setup
6. Komodo
7. 다른 분야에의 적용
8. ASIC 마이너 개발
9. 사건사고
   9.1. 취약점 발견
10. 관련 문서


## 1. 개요

**Zcash**는 Zerocoin 프로젝트에서 파생된 암호화폐이다. 암호화폐 사용자들의 익명성을 높이기 위한 목적으로 만들어졌다.

Zerocoin 프로토콜은 향상된 후 Zerocash로 발전하였고, 이 Zerocash가 2016년에 Zcash가 되었다. Zcash의 설립자 겸 CEO는 Zooko Wilcox-O'Hearn이다. 존스 홉킨스 대학교의 Matthew D. Green이 암호학자로 참여하였다.

한국 거래소에서는 익명성을 이유로 전부 상장폐지되었다.

비슷하게 익명성을 중시한 암호화폐로는 모네로, Dash 등이 있다.

## 2. 주소 유형

https://zechub.wiki/guides/using-zec-privately
https://ywallet.app/getting-started/private_tx/

Zcash의 주소는 Transparent, Sapling, Orchard 총 3가지 유형이 있다. Transparent는 공개적이고 Sapling과 Orchard는 비공개적이다. 주소의 첫문자는 Transparent는 t, Sapling은 z, Orchard는 u이다.

쉬운 이해를 위해 일단 Transparent와 Sapling만 생각하고 Orchard는 생각하지 않는다.

Transparent(t-Address)를 통한 거래는 비트코인처럼 공개적이고 Sapling(z-Address)을 통한 거래는 비공개적이다.
나와 상대방이 2가지 유형의 주소 중 하나를 선택한다면 Zcash 거래 유형은 총 4가지이다.

| 송신유형 | 발신자 숨김 | 수신자 숨김 | 금액 숨김 |
|---|---|---|---|
| z2z | O | O | O |
| z2t | O | X | X |
| t2z | X | O | X |
| t2t | X | X | X |

거래소에서 구한 Zcash를 개인지갑의 z-Address로 옮기는 방법에는 2가지가 있다.
1. 거래소 -> 개인지갑(z-Address)
2. 거래소 -> 개인지갑(t-Address) -> 개인지갑(z-Address)
만약 거래소가 z-Address로의 출금을 허용하지 않는다면 먼저 t-Address로 출금한 뒤 z-Address로 옮기면 된다.

Orchard는 최신 차폐형 풀(Shielded Pool)로 Sapling을 서서히 대체하고 있다.

## 3. 지갑 소프트웨어

https://z.cash/ecosystem/?wallets=#tag-wallets
https://zechub.wiki/wallets
https://ywallet.app/installation/ - YWallet
https://www.zingolabs.org/ -Zingo 모바일
https://github.com/zingolabs/zingo-pc - Zingo 데스크탑[1]

Zcash를 저장할 수 있는 개인지갑에는 여러 가지가 있다. 이 중 'Shielded by default'이면서 더불어 최신 차폐형 풀(Shielded Pool)인 Orchard를 지원하는 지갑은 YWallet과 Zingo뿐이다.
해외 Zcash 커뮤니티에서는 YWallet을 주로 사용하는 것으로 보인다.

만약 윈도우에서 YWallet을 설치한다면 ZIP는 지갑을 생성할 수 없는 오류가 있으므로 마이크로소프트 스토어에서 설치해야 한다.

데스크탑 YWallet의 설정에서 Advanced Mode를 켜면 새 주소를 만드는 'New Snap Address' 버튼을 활성화할 수 있다.

만약 Tails OS에서 YWallet이나 Zingo를 AppImage를 이용해 설치하고자 한다면, 이 링크를 참고할 수 있다. 지갑은 다르지만 과정은 똑같다.

## 4. 익명성

> "Zcash, I have said repeatedly, really does the best in the space with their shielded transactions. The criticism is that these transactions don't occur by default, which is valid. In my opinion, they should happen by default. There are other cryptocurrencies like Monero, which is having a lot of trouble being listed on exchanges broadly, whic

> h has sort of privacy by default, but it's a lower measure of privacy. **You're just playing a shell game and those shell games don't really last forever.**"
> "내가 반복해서 말했듯이 Zcash는 보호된 거래를 통해 이 분야에서 정말 최고의 성과를 내고 있습니다. 비판은 이러한 거래가 기본적으로 발생하지 않는다는 것입니다. 이는 유효합니다. 제 생각에는 이러한 일이 기본적으로 발생해야 합니다. Monero와 같은 다른 암호화폐도 있는데, 이는 거래소에 광범위하게 상장되는 데 많은 어려움을 겪고 있습니다. 기본적으로 일종의 개인 정보 보호 기능이 있지만 개인 정보 보호 수준은 낮습니다. **당신은 단지 셸 게임을 하고 있을 뿐이고 그 셸 게임은 실제로 영원히 지속되지는 않습니다.**"
>
> 에드워드 스노든 🔗 #
> 모네로의 원리에 대해 알아보면 이 야바위 비유가 얼마나 적합한지 알 수 있다.

> 모네로의 링 서명은 실제 거래에 10개의 가짜 거래를 섞어 누가 실제 거래자인지 모르게 합니다. 이는 자신이 진짜 거래자가 아님을 주장할 수 있는 그럴듯한 거부 가능성(Plausible deniability)을 만드는 역할을 합니다.
>
> 🔗 https://archive.md/4rpx5

오류가 발생했습니다.

www.youtube.com에서 동영상을 시청하거나 브라우저에서 자바스크립트가 사용 중지된 경우 사용 설정하세요.

영 지식 증명에 대한 유튜브 동영상이다.

🔗 Keepit 블록체인 칼럼: 익명화폐의 역사 3편
🔗 https://zechub.wiki/guides/zero-knowledge-vs-decoys

영 지식 증명(zero-knowledge proof) 기술을 사용한다. 영 지식 증명이란 A와 B가 거래를 할 때 private key를 보여주는 대신에 연속적으로 질문을 던져 그것을 다 맞히면 맞다고 인정을 해주는 것이다. 그러면 정보의 제공이 최소화되므로 추적이 힘들어진다.

## 5. Trusted Setup

🔗 https://www.coindesk.com/tech/2022/05/31/zcashs-nu5-upgrade-goes-live-boosting-privacy-and-removing-trusted-setups/
🔗 https://www.reddit.com/r/zec/comments/90zkhb/what_is_trusted_setup_and_why_is_it_a_problem/

한때 Trusted Setup이라는 문제가 있었다. 현재는 업그레이드되면서 Trusted Setup을 제거하여 문제가 해결되었다.

## 6. Komodo

Komodo는 지캐시에서 포크되서 나온 코인이다.

아토믹 스왑과 코모도에 대한 글이다. 🔗 [KMD] 아토믹 스왑(Atomic swap)에 대한 모든 것 (feat. Komodo)|#

## 7. 다른 분야에의 적용

암호화폐이자 스마트 컨트랙트 플랫폼인 Ethereum과 Tezos에 Zcash의 익명화 기술이 적용될 예정이다.

JP모간 체이스에서 Zcash의 익명화 기술을 Quorum블록체인에 적용하였다.

## 8. ASIC 마이너 개발

Bitmain에서 Zcash의 ASIC 마이너를 개발했다고 한다.

🔗 Crypto Hardware Giant Bitmain to Release First Zcash ASIC Miner (MAY 03, 2018)
🔗 Bitmain launches the Antminer Z9 mini to mine Zcash [ZEC] (May 4, 2018)

## 9. 사건사고

### 9.1. 취약점 발견

2026년 6월경 지캐시의 취약점이 발견되었다. 이 버그를 사용하면 지캐시를 **무한 위조 발행**하는 것이 가능했는데 해당 취약점은 무려 4년동안 발견되지 않고있었다. 취약점은 긴급 패치를 통해 빠르게 수정되었지만 지난 4년간 누군가 버그를 악용하여 위조발행을 했는지 확인할 방법이 없었다. 이 소식이 알려지자 지캐시는 50% 가까이 폭락하였으며 아서 헤이즈는 이 소식이 전해지자 자신의 지캐시를 전량 매도하였다.

🔗 https://biz.sbs.co.kr/article/20000316715

## 10. 관련 문서

- 모네로
- 암호화폐 거래소

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.